巨峰云平台(蜂云平台)安全白皮书

JuFeng BCloud Information Security White Paper

Version 1.0.202105

目录

1. 蜂云平台介绍

1.1 巨峰介绍

杭州巨峰科技有限公司成立于 2008 年，是一家以“研发”为核心，集生产、销售、服务于一体的高新技术企业，致力于提供高品质、高性价比的安防产品和行业解决方案。公司总部位于杭州市富阳区银湖创新中心，经多年发展，巨峰已成为国内拥有优良口碑的视频监控产品及解决方案提供商，目前在国内各大城市设立分支机构，辐射全国，服务于广大客户。

巨峰科技自成立以来一直专注于视频安全领域，拥有自主知识产权的核心技术和解决方案。同时不断挑战新技术新方法。公司主要提供网络摄像机、硬盘录像机、网络视频服务器、视频编解码器、智能家居、拼接屏、云监控平台等视频监控全线设备与整体行业解决方案，涵盖道路监控智能交通、城市安防、车载监控、小区监控、物联网等众多领域。产品畅销海内外市场，出口多个国家，让世界各地的客户得以体验巨峰带来的快捷和便利。

巨峰科技凭借具前瞻性的创新技术，成为业内具有超凡发展潜力的高新技术企业。公司拥有专利、软著、商标等多项独立知识产权和相关资质证书，被认定为杭州市企业技术中心和杭州市高新技术企业研发中心并荣获中国安防网百强企业称号，是中国平安城市建设推荐品牌和中国安全防范产品行业协会会员之一，被列入国家级高新技术企业。公司产品获得杭州市重大科技创新项目立项、浙江省级工业新产品称号。公司同时获得浙江省安全技术防范行业资信等级证书。

1.2 巨峰云平台（蜂云平台)介绍

巨峰云平台（蜂云平台）伴随着公司安防监控产品应运而生，为巨峰及其客户提供安全、稳定、快速的视频云服务。巨峰云平台在全球部署云服务，拥有千万级用户用户和亿级并发处理能力。同时巨峰云平台为客户和厂商提供了自助软件开发的 SDK 与开放完善的云平台 API。同时提供调试 Demo，可最大限度地降低厂家的开发门槛，节约开发成本，提升厂商的只能产品研发速度。同时还能够帮助厂商进行软硬件升级，持续为最终消费者提供优质的服务。

巨峰云平台（蜂云平台）是一个同时面向终端消费者（toC）和企业客户（toB）的统一平台，基于巨峰及其合作伙伴常年的经验积累和总结，不断优化，针对不同的客户群体统一基础云平台服务，极大的便利了厂家业务拓展的可持续性和兼容性。

1.3 信息安全保障的使命

巨峰致力于为客户提供一致、安全、可靠并且符合法律要求的视频和 IoT 接入服务，切实地保障客户及其用户的数据的可用性、机密性和完整性。巨峰云承诺：巨峰云平台（蜂云平台）以数据保护为核心，以云安全能力为基石，依托巨峰独有的物联网解决方案，打造业界领先的竞争力，构建完善的云平台安全保障体系，并一以贯之的将信息安全保障作为巨峰云的重要发展战略之一。

为了达到这些目标，我们实现了各个层面的安全防护包括对外所有服务的安全检查、安全防御以及安全监控和审计，形成事前、事中、事后的全过程防护。

这篇白皮书从以下方面讨论了蜂云平台的各种安全防护措施：

1. 安全责任
2. 合规性
3. 数据安全
4. 云平台基础架构
5. 安全组织和人员
6. 云平台安全保障
7. 安全开发周期管理
8. 安全运维和运营
9. 业务安全和风控
10. 终端安全
11. 业务可持续性

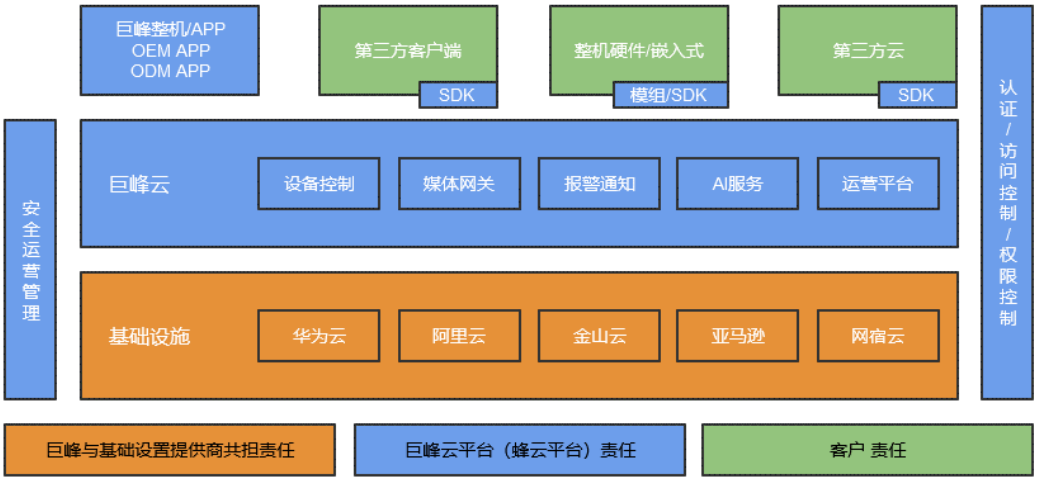
该白皮书致力于让客户更加全面、系统的了解巨峰云（蜂云平台），并对巨峰云平台有更深入的安全洞察。

“巨峰云平台（蜂云平台）”以下简称“蜂云平台”。

2. 安全责任

巨峰负责蜂云平台上的服务和数据交互的安全管理和运营，对提供的云服务平台和基础架构的安全性负责。客户自行开发 App 或者硬件嵌入式软件接入蜂云平台需要客户自己保障其应用及数据，包括硬件和 App 的安全合规。

下图为基础云服务商、巨峰以及客户信息安全责任共同承担责任模型：



2.1 蜂云平台的安全责任

蜂云平台通过选择全球知名的云主机服务商亚马逊、华为云、阿里云等全球一流云平台，确保安全管理和运营的基础设施和基础网络安全。

蜂云平台安全覆盖数据安全和云服务安全。巨峰承诺利用其安全团队以及全球范围内知名的安全服务厂商的专业攻击防护技术经验，提供云平台的安全运维和运营服务，切实保护巨峰云的安全运营，以及保障客户、用户隐私和数据的安全。主要覆盖但不限于如下：

- 数据安全：指客户在云计算环境中的业务数据自身的安全管理，包括收集与识别、分类与分级、权限与加密以及隐私合规等方面；
- 访问控制管理：对资源和数据的访问权限管理，包括用户管理、权限管理、身份验证等；
- 云服务安全：指在云计算环境下的业务相关应用系统的安全管理，包括应用和服务接口的设计、开发、发布、配置和使用等方面。

2.2 客户的安全责任

客户在使用蜂云平台的解决方案的时候，需要严格按照巨峰的安全配置和接入要求执行。同时客户需要保证自己的云端、客户端或者硬件产品本身的安全性。基于巨峰 SDK 开发的 APP，巨峰仅提供技术支持，但是无法提供任何安全保障。对于基于巨峰 OEM(公版)APP(无任何定制场景)的数据安全合规、隐私政策等相关信息，巨峰会提供模板供客户参考，具体上线的隐私政策声明以及法律合规性由客户自己负责，必要时候，巨峰安全团队愿意提供安全解决方案的帮助和咨询

服务。

3. 合规性

巨峰遵守国际权威的安全标准及行业要求，并整合到内部控制框架中，在云平台、APP、硬件产品等需求实现过程中严格执行。巨峰与独立第三方安全服务、咨询和审计机构进行合作，验证和保障了蜂云平台的合规性和安全性。目前，巨峰已经通过全球多个咨询和审计机构的信息安全和隐私合规的认证，是一家拥有多个认证的 IoT 解决方案提供商。巨峰承诺，将持续地进行多个信息安全和隐私安全相关的认证和合规证明，为客户的数据和隐私安全保驾护航。

目前，我们的认证和合规凭证如下所示：

3.1 ISO 9001

巨峰云（蜂云平台）已获得 ISO 9001 认证。

ISO 9001 是由全球第一个质量管理体系标准 BS 5750（BSI 撰写）转化而来的，ISO 9001 是迄今为止世界上较为成熟的质量框架。它是一个系统性的保证公司产品质量及运作的指导性纲领和规范架构，围绕企业提供的产品或服务展开。策划和实施及改进产品或服务实现的全过程，确保满足客户及相关法律法规要求。运用质量管理系统，能够有效和高效地实现预期的质量目标。通过对质量管理体系的审核和管理评审，采取纠正措施和预防措施。持续改进质量管理体系的有效性，是企业发展与成长的根本。

3.2 ISO 27001

巨峰云（蜂云平台）已获得 ISO 27001 认证。

ISO 27001 是信息安全管理体系（ISMS）国际标准，为各类组织建立并运行信息安全管理体系提供了最佳实践指导。按照标准要求：

- 基于业务风险的方法，建立、实施、运行、监控、评审、维护和改进信息安全；
- 为了确保信息的机密性、完整性和可用性，设立了相应的组织架构，建立了体系化的安全管理制度，并提供资源保障；
- 遵循 PDCA 方法，持续改进信息安全管理。

4. 数据安全

4.1 数据安全体系

巨峰云数据安全体系从数据安全生命周期角度出发，采取管理和技术两方面的手段，进行全面、系统的建设。通过对数据生命周期（数据收集、存储、加工、传输、共享、删除）各环节进行数据安全管理管控，实现数据安全目标。

在数据安全生命周期的每一个阶段，都有相应的安全管理制度以及安全技术保障。

4.2 数据所有权

巨峰为客户定制的服务中，客户是数据控制者，客户需要保证数据使用的合规性，巨峰是数据处理者，巨峰将在符合法律法规的基础上按照客户书面指示、合同约定来处理客户个人数据，所有数据处理行为对客户透明。因此，在符合法律法规、《隐私政策》的基础上，巨峰可帮助客户和用户保障数据的保密性、完整性、安全性。

4.3 多副本冗余存储

采用分布式架构，所有业务服务器同时部署于同城不同区域的三个机房，数据库等数据存储服务采用多副本模式(最少保证二个实时副本)，并实时进行数据

备份。从物理层面保障了数据和服务的高可靠性和高可用性。

4.4 用户设备数据安全

用户设备序列号随着用户系统统一保存，只有用户密码校验正确时才能获取。

手机客户端设备密码在用户输入后仅会保存在当前客户端本地，不会同步或上传到云端，不存在设备密码在云端被泄露的可能。

云网站为了使用方便，会有“记住密码”的功能，完全有用户自愿编辑和保存，保存之后用户可以随时进行清除和修改操作。

设备端和客户端的信令数据交互，云端不做解析或数据保存。

设备端和客户端的视频交互数据在云服务器内存内会做短暂保存，若干秒后会自动释放。

4.5 残留数据清除

蜂云平台使用过的云主机，一旦释放和回收，其所有信息将被自动进行零值覆盖。同时，任何更换和淘汰的存储设备，都将由云服务器基础设施提供方统一执行消磁处理并物理销毁之后，才能运出数据中心。

4.6 隐私保护

蜂云平台践行“一切以用户价值为依归”的经营理念，尤其重视与客户建立长久持续的信任关系。巨峰以坚实的技术基础和完备的运营管理机制，确保用户和客户数据得到全面的保障。巨峰云将严格执行巨峰公开发布的《隐私政策》，切实保护用户隐私。

云平台对隐私数据的主要保护手段如下：

- 隐私数据生产和分类
  - 基本原则：
    - 信息收集主体的所有行为的合法要求，包括数据主体的授权和法律责任的明确。
    - 收集的数据最小化原则，不收集和提供的服务无关的数据。
  - 充分的用户知情权，
    - APP 和网站的隐私政策
      - 隐私条款必须明确应用收集的所有用户数据类型及与之相对应的服务。
      - 隐私条款必须在涉及注册、更新等重要时机通过邮件、APP 弹窗等方式告知用户。
      - 隐私条款必须包含数据收集、删除、迁移、保存、用户选择权等。

- 要求用户必须对隐私政策作出反馈。
- ◆ 网站 Cookie 声明
  - Cookie 的作用及用户选择权。
- ■ 用户权限：
  - ◆ 访问权
    - 巨峰用户可通过 App 访问巨峰收集的个人数据，无需另外技术支持。
    - 巨峰用户可请求巨峰告知对其数据的处理和使用情况，
  - ◆ 被遗忘权（数据删除权）
    - 账号注销权限和删除数据
  - ◆ 纠正权
    - 若得知用户主动提供的个人信息存在不准确或需及时更新的情况，用户可在 App 上手动修改。
  - ◆ 可携带权
    - 用户通过巨峰 APP 反馈或者客户邮箱反馈，要求将提供给巨峰的个人数据传输给另一个数据控制者。
- ■ 数据分类：区分个人数据和平台信息数据，针对个人数据，需要用敏感程度分类。

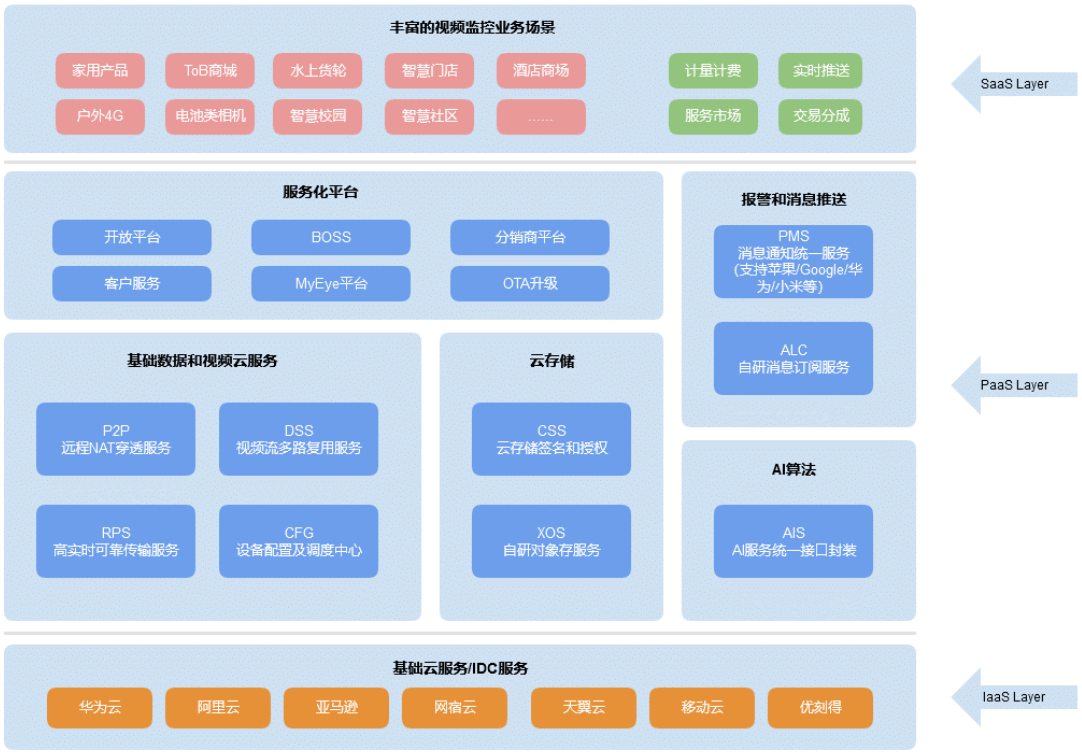
4.7 数据存储区域

全球四大集群：中国大陆地区、南北美及加勒比海地区、欧洲非洲区、亚太地区（含中国香港/中国澳门/中国台湾）。根据用户所在地区就近提供相应的数据服务。

- 中国大陆地区：数据保存在华为云-广州/华为云-北京四/华为云-上海二机房，由华为云提供基础云计算服务；杭州机房由阿里云提供云计算服务；扬州机房由网宿云提供云计算服务；
- 南北美及加勒比海地区：美国西部-俄勒冈机房/加利福尼亚机房和美国东部-弗吉尼亚北部机房，由亚马逊（美国）提供云计算支持；南美-巴西圣保罗由亚马逊和华为云共同提供云计算基础服务；
- 欧洲非洲区
  - ■ 欧盟国家：德国法兰克福机房，由亚马逊提供计算服务；
  - ■ 俄罗斯：由华为云和俄罗斯运营商 Sbercloud 合营机房共同提供云计算基础服务；
  - ■ 南非：约翰内斯堡机房，由华为云提供云计算基础服务；
- 亚太地区：新加坡/香港/印度/泰国/越南/菲律宾等机房，由亚马逊/华为云/网宿云/优刻得等共同提供基础云计算服务；

5. 云平台基础架构

5.1 云平台基础架构图



蜂云平台的基础设施由华为云、亚马逊等提供，整合了全球服务节点。在服务层面，为客户和厂商提供了自助式软件开发 SDK 与开放完善的云平台 API。

详见开放平台：https://open.bcloud365.net。

5.2 云服务器供应商要求

巨峰选择云服务器供应商要求：

1. 全球知名云服务提供商品牌，技术水平全球领先。
2. 云计算产品安全和稳定。
3. 拥有和符合全球范围内最完备的信息安全合规、法律和资质证明。

目前被我们选择的云服务器提供商，包括华为云、亚马逊、阿里云等。

6. 安全组织与人员

6.1 安全与隐私保护团队和人员

巨峰内部成立了安全委员会，由关键创始人带领委员会，成员来自市场部/人力资源部/研发部等各部门骨干人员，以遵守法规和合规性要求为基线，为巨峰（包括运营和业务利益相关方）提供风险和合规性支持。

安全委员会下辖网络安全技术中心和安全应急响应中心两个部门。

6.2 人力资源管理

巨峰的人力资源管理框架和公司的整体人力资源管理框架一致，都是建立在法律基础之上。安全对 HR 的诉求主要是保证我们的员工背景和资历适合巨峰业务的需要。员工行为符合所有法律、政策、流程以及巨峰商业行为准则的要求。员工有履行其职责必备的知识、技能和经验。

员工离职，会有严格的内部 Task 系统流程，各个环节有责任人对于其电子设备、服务器、各种账号等资源的回收或销毁，否则无法完成离职手续的办理。

6.3 安全意识教育

为了提升全员的网络安全意识，规避网络安全违规风险，保证业务的正常运营，巨峰内部发布了《网络安全技术中心制度》和《网络安全技术中心操作规程》，公司同时也颁布了《保密制度》，并以此为基准定期开展网络安全意识教育学习，要求员工持续学习网络安全知识，了解手册上面的的政策和制度。知道哪些行为是可以接受，哪些是不能接受的，意识到即使主观上没有恶意，也要对自己的行为负责，并承诺按要求执行。

6.4 安全管理体系相关培训

为了让公司全员能够准确理解公司信息安全管理政策，并且有效推动和落实安全策略，每年公司安全团队和法务团队进行《保密制度》等公司信息安全的培训。

6.5 信息安全能力提升

巨峰内部会定期的举行安全开发培训和信息安全交流，旨在提升员工的安全技能，确保员工有能力交付安全、合规的产品、解决方案和服务。

7. 云平台安全保障

7.1 物理安全

7.1.1 高可用的基础设施

巨峰云平台整合全球最知名的云主机服务商亚马逊、阿里云和华为云等，构建全球服务节点。为客户提供安全、稳定、持续、可靠的物理设施基础。

巨峰云根据中国企业内外销区域结合海底光缆分布和全球各城市的实测结果,部署覆盖中国大陆地区、欧洲、非洲、美洲和亚太地区等可用区。

- 中国大陆地区：
  - 华为云（包括但不限）：
    - 华北-北京一机房
    - 华北-北京四机房
    - 华东-上海一机房
    - 华东-上海二机房
    - 华南-广州机房
    - 西南-贵阳机房
  - 金山云（包括但不限）：
    - 北京六区
  - 阿里云（包括但不限）：
    - 华东一（杭州）机房
    - 华东二（上海）机房
  - 网宿云（包括但不限）：
    - 扬州机房
  - 天翼云（包括但不限）：
    - 杭州
    - 苏州
    - 广州
    - 北京
    - 成都
  - 移动云（包括但不限）：
    - 杭州
    - 广州
    - 北京
    - 成都

- 亚太地区（包括港澳台）：
  - 华为云（包括但不限）：
    - 亚太-香港
    - 亚太-泰国

- 亚太-新加坡
- 亚马逊（包括但不限）：
  - 亚太地区-东京
  - 亚太地区-新加坡
  - 亚太地区-香港
  - 亚太地区-孟买
  - 亚太地区-首尔
  - 亚太地区-悉尼
- 欧洲：
  - 亚马逊（包括但不限）：
    - 欧洲-法兰克福
    - 欧洲-爱尔兰
    - 欧洲-斯德哥尔摩
    - 欧洲-米兰
    - 欧洲-巴黎
    - 欧洲-伦敦
  - 华为云（包括但不限）：
    - 俄罗斯（Sbercloud 合营）

- 非洲：
  - 华为云（包括但不限）：
    - 南非-约翰内斯堡
  - 亚马逊（包括但不限）：
    - 南非-开普敦

- 美洲：
  - 亚马逊（包括但不限）：
    - 美国西部-加利福尼亚北部
    - 美国西部-俄勒冈
    - 美国东部-弗吉尼亚北部
    - 美国东部-俄亥俄
    - 拉美-圣保罗
  - 华为云（包括但不限）：
    - 拉美-圣保罗
    - 拉美-圣地亚哥
    - 拉美-墨西哥-

7.1.2 安全审查和审计

安全事件管理：和云服务器供应平台达成物理安全应急预案，并定期组织数据中心工作人员进行安全演练。一旦发生物理安全事件，该预案将能够立即生效并指导相关人员以最大可能保护客户资产。

7.2 网络安全

7.2.1 DDoS 防护

巨峰云使用华为云、亚马逊、阿里云等云平台的 DDoS 防护功能保护所有数据中心，自动检测、调度和清洗，保证云平台网络稳定。
同时内部通过异常 IP 自检的方式，对非正常业务请求的来源 IP 做主动隔离，动态屏蔽可疑的源地址。

7.2.2 入侵防护

- 入侵检测：部分关键服务器购买华为云、亚马逊等云平台的安全防护功能（Web 防火墙 WAF 和云防火墙 CFW）；
- 主机监控：所有服务器上都按照部署了自研的监控程序，对 CPU/内存/带宽/磁盘等使用情况做实时监控，并保留 3 天的实时运行数据；运维平台可配置以下预警：
  - 资源使用率超过预置阀值预警（所有服务器的 CPU/内存/磁盘/带宽）
  - 带宽出入网差值过大预警（主要应用于视频流服务器）
- 数据库审计：对数据库的权限进行严格的统一管理和限制，并且对所有数据库的增删改查都进行了完备的日志审计；每天至少定时全量备份数据库一次。

8. 安全开发管理

8.1 安全需求分析和产品设计

产品设计阶段，安全技术中心对系统进行攻击面分析、威胁建模，对产品设计中采用的技术进行安全评估，，并与开发人员就安全建议达成共识。

8.2 开发阶段

开发阶段，要求开发人员严格遵循安全编码规范，对开发人员在编码中出现的安全风险进行提醒。代码提交之后，相应人员严格进行代码评审，才允许合并到正式代码分支；如果由安全问题，通知对应开发进行安全修复。

8.3 安全测试和修复验证

在产品测试阶段，针对已知的漏洞，安全中心测试人员会对数据交互网络包进行抓包分析；对设备进行端口扫描，如果有已知漏洞未修复的，测试退回并重新修复验证。

9. 安全运维和运营

通过巨峰云的安全运维平台进行统一的管理，采取严格的访问控制、监控审计来确保运维安全。

账号管理和身份认证：使用公司内部 Task 的账号管理和身份认证系统管理员工账号生命周期，每个员工存在唯一的账号；确保只有公司在职员工才有访问运维平台的可能。另外并非所有在职人员都能访问运维平台，还需网络安全中心负责人进行授权。

授权：由网络安全中心负责人对账号进行权限授权，制定查看或操作运维平台的部分内容。

监控：巨峰云使用自动化监控系统对云平台网络设备、服务器、数据库、应用集群以及核心业务进行全面实时监控。监控系统广泛使用仪表盘展示巨峰云关键运营指标，并可配置告警阈值，当关键运营指标超过设置的告警阈值时，自动通知运维和管理人员。

9.1 客户安全服务支持

公司官网提供的专门的网络安全板块，包含“安全公告”和“漏洞上报”，并提供 7x24 小时客户服务热线。

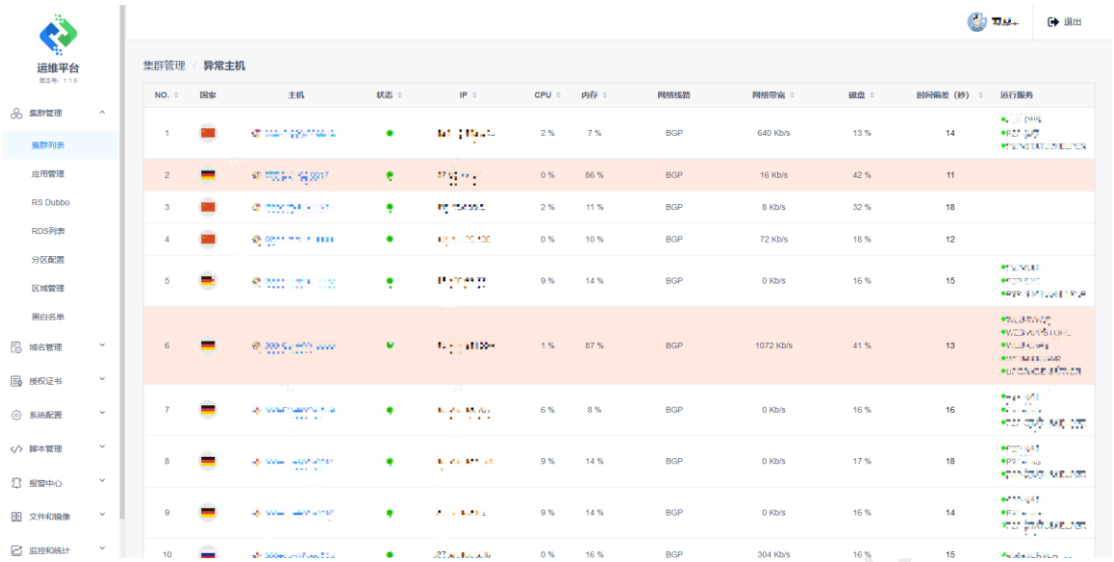
9.2 运维平台告警

运维平台值守分人工值守和机器人异常捕捉主动预警两个部分。

9.2.1 人工值守

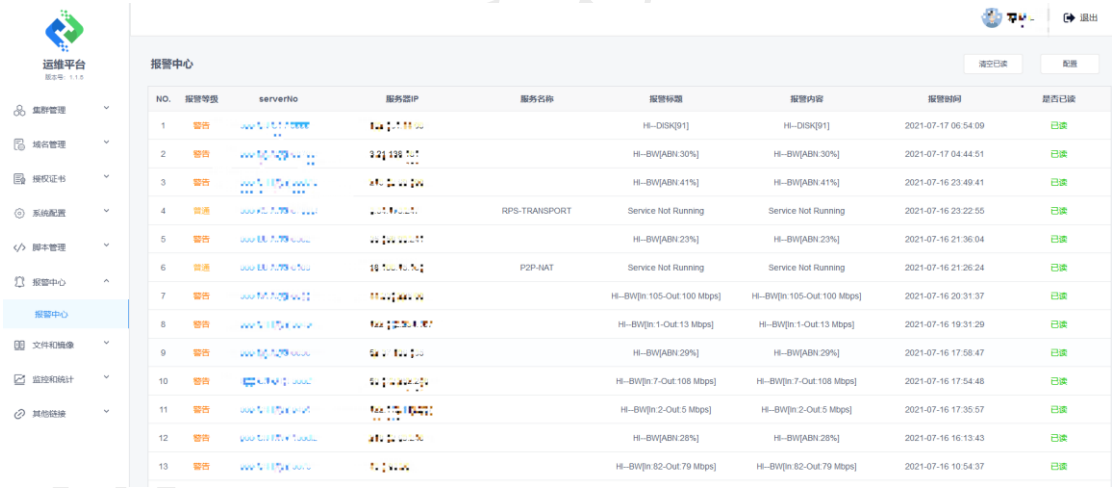
人工值守值班人员每天需要核对《云平台运维日常清单(Checklist)》排查一遍云平台所有业务服务器；主动分析平台异常服务器的状态，分析异常和故障原因。

下图是运维平台异常主机列表，每天由值班人员分析并处理：



9.2.2 机器人预警

运维平台自动分析云主机异常行为并实时触发告警，告警消息会同时以钉钉机器人和微信服务号的方式通知到运维管理人员，并第一时间处理解决。



钉钉机器人和微信服务号实时报警通知：

10. 业务安全与风控

10.1 账号安全

账号安全是巨峰云服务体系的基础，所以针对账号的注册、登录、密码找回、多设备登录等都进行了严格的安全管控和日志审计。同时，针对账号体系的数据存储、查询和修改都进行了严格的保护。针对撞库、API 滥用等常见账号风险来源进行严格的策略保护。

同时，对用户注册时候，弱密码的检查，禁止常见弱密码的设置。

10.2 内容安全

所有业务数据均有特定业务授权码，只有账号登陆正常时才会下方对于的业务授权码，并且授权码时动态的，对终端提交的内容进行数据校验，减少安全风险。

11. 终端安全

11.1 App 客户端

所有 App 客户端均由唯一 AppKey，并且申请对应的 App 密钥才允许使用。当系统检测到 App 出现恶意请求时，平台可以终止此 App 客户端的所有数据请

求。

11.1.1 客户端程序保护

客户端本身的安全往往是黑客突破 APP 客户端安全的第一道坎。从黑盒的思路，攻击者需要拿到客户端的源代码，然后对代码进行快速解读，包括查找特点的关键字或方法等，寻找漏洞。所以需要在这个过程增加一道门槛。除此之外，保护应用包不能被二次打包也是非常重要的手段。APP 客户端保护，包括针对客户端防篡改、代码混淆、模拟器检测拦截、Root 环境检测告警、防止调试、界面劫持保护、Hook 插件检测和进程注入保护等。

11.1.2 组件安全

针对四大组件，Activity、Broadcast Receiver、Service、Conent Provider，严格限制组件的使用权限和访问权限，同时针对对外开发的组件，进行严格的权限和输入校验。针对 WebView，保持 SDK 较高版本，针对 URL 域名和 file 访问权限进行严格控制。

11.1.3 数据安全

APP 客户端针对存放在客户端本地的数据，进行了严格的控制。

1. 内部存储：
   a) 私有目录：本地部分必须存放的配置文件等信息，通过安全的加密方式保存，同时密钥每个用户唯一，同时采用严格的读写执行权限设置。
   b) 安卓的 SharedPreferences 配置文件：不允许出现敏感信息。
2. 系统日志：正式的客户端不打印和存放任何交互 logcat 或日志文件。
3. 密钥链数据：不硬编码重要的 Key。采用自主研发的安全算法保存密钥。
4. 内存数据：重要操作时候，用户数据不存入内存。

11.1.4 通信安全

- SSL 加密支持，HTTPS 支持；
- 设备交互数据 RSA+AES 加密支持；
- 视频流私有加密支持；

11.2 硬件和固件安全

11.2.1 通信安全

根据不同 CPU 主控芯片，巨峰提供不同等级的加密机制，最大化芯片的

安全防护，不论哪种加密机制均保证数据的通信安全。目前 NETIP 私有加密协议和 HTTPS，同时针对交互过程中的数据和控制指令进行额外的 AES 加密保护。基于 MD5，真随机数等加密算法生成的基于设备的，具有唯一性的随机密钥。

同时，巨峰所有通讯数据都会使用防重放校验、设备身份校验、访问控制和权限校验等多种数据保护机制

11.2.2 固件保护

巨峰针对固件进行多重保护机制：

1.固件 flash 读写保护，根据芯片的平台支持程度，对固件的读写进行限制，防止通过硬件进行固件读取和写入，同时防止设备系统固件被恶意修改；

2.固件加密保护，部分平台本身支持固件加密，巨峰均会启用；

3.固件防伪校验，巨峰固件都会通过巨峰的证书进行签名；

4.代码混淆，对核心的代码进行额外的混淆和保护，特别是加密模块。

11.2.3 OTA 安全

1.可信启动，巨峰会根据芯片平台的能力进行固件防篡改保护，对核心系统或全部固件的启动校验。

2.可信升级，设备升级固件时，升级服务器对固件进行可信验证，拒绝非法或篡改的固件写入设备，同时设备先完全下载后，先对整个升级固件的合法性和完整性进行全部校验，才开始正式升级；

3.可信执行，设备运行期间，任何执行程序在加载运行前，均需通过内核的可信验证，避免恶意程序执行，入侵设备。

11.2.4 数据保护

- 用户数据保护
  利用加密技术对用户数据进行保护，用户数据主要包括用户配置数据和用户隐私数据，数据加密，防止数据费被强制拷贝走后被攻击者破解。用户数据主要指配置参数，使用信息，不包括人脸对比图片，模型等。

- 存储介质加密
  支持对于各类存储介质上的各种数据进行加密，避免数据泄露，尤其是可插拔存储介质上的关键数据（音频视频数据）进行加密等
- 数字水印
  数字水印是一种信息隐藏技术，它的基础思想是在数字图像，音频和视频等数据产品中嵌入加密信息，保护数字产品的版权，证明产品的真实性和可靠性。数字水印提供了一种隐藏标识的方法，标识咋原始文件上是看不到的，只有通过特殊阅读程序才可以读取，在视频流添加数字水

印可以解决视频被篡改攻击的理想途径，通过水印可以判断视频信息是否给篡改。

11.2.5 配网安全

配网前的 wifi 设备发现，APP 和硬件发出的广播信息，经过 AES 加密等的传输。

配网过程中，APP 采用 AES 加密传输给硬件 WIFI 信息，保障了用户网络的安全，减小配网过程的风险。

12. 业务可持续性

12.1 业务持续性

为消除关键的生产经营活动出现中断，避免其遭受重大故障或灾难的影响，通过运维平台对云平台所有的主机、应用、服务、网络等的实时监控，并且有一套完整的业务故障的自动化流程体系和保障，通过多服务热切换保障服务不中断。

针对业务系统软件硬件故障甚至天灾等非抗拒性因素导致的风险，规定了一套完整的应对方案，有能力保证在预知情况下的业务持续性。

12.2 灾难恢复

采用主从数据实时热备份、冗余存储和地备份的方式，保障业务数据安全可靠，持续可用。并对对备份情况进行实时的监控和验证。同时针对业务系统，多链路备用系统，保证能够快速应急切换。

12.3 应急方案

运维团队内部建立对各类型资产和安全风险的应急方案措施，能够保障事后能够正确、有序、高效地进行应急处理，保障工作的正常运转。应急方案包括了事前的预案流程、监控和一系列故障应对手段。事中通过详细的系统监控审查记录，为事后提供足够资料能够快速了解和分析，以及对应的接口人员。事后有一套完善的处理流程方法和应急预案，保障能够快速处理问题，分析问题和责任追责。

12.4 应急演练

定期实施大型的硬件故障、网络 DDoS、安全事件等内部技术应急演练测试和实战。